Printing Requisition / Graphic Services 33

Dept. No. 46068

Title or Description CS-78-32

Date May 28/79 **Date Required** **Account** 126-6240-41

Signature **Signing Authority**

Department Comp. Sci. **Room** 5100 **Phone** 3293 **Delivery** □ Mail □ Pick-up □ Via Stores □ Other

1. Please complete unshaded areas on form as applicable. (4 part no carbon required).
2. Distribute copies as follows: White, Canary and Pink—Printing, Arts Library or applicable Copy Centre Goldenrod—**Retain.**
3. On completion of order, pink copy will be returned with printed material. Canary copy will be costed and returned to requisitioner, **Retain as a record of your charges.**
4. Please direct enquiries, quoting requisition number, to Printing/Graphic Services, Extension 3451.

Reproduction Requirements ☑ Offset □ Signs/Repro's □ Xerox **Number of Pages** 36 **Number of Copies** 25

Type of Paper Stock ☑ Bond □ Book □ Cover □ Bristol □ Supplied

Paper Size ☑ 8½ x 11 □ 8½ x 14 □ 11 x 17

Paper Colour ☑ White □ Other **Ink** ☑ Black

Printing ☑ 1 Side □ 2 Sides **Numbering** to

Binding/Finishing Operations ☑ Collating □ Corner Stitching □ 3 Ring □ Tape □ Plastic Ring □ Perforating

Folding Finished Size **Cutting** Finished Size

Special Instructions covers attached

Cost: Time/Materials	Fun.	Prod.Un.	Prod. Cl.	Opr. No.	Mins.	Total
Signs/Repro's	1					
Camera	2					
Correcting & Masking Negatives	3					
Platemaking	4					
Printing	5		33		25	
				HK	30	
Bindery	6					
Sub. Total Time						
Sub. Total Materials						
Prov. Tax						
Total						

Film Qty Size **Plates** Qty Size & Type

Paper Qty Size **Plastic Rings** Qty Size

Outside Services

Languages of $\mathcal{R}$-Trivial Monoids[†]

by

J. A. Brzozowski and Faith E. Fich
Department of Computer Science
University of Waterloo
Waterloo, Ontario, Canada
N2L 3G1

Research Report CS-78-32
July 1978

[†] This research was supported by the National Research Council of Canada under a postgraduate scholarship and under grant No. A-1617.

Languages of $\mathcal{R}$-Trivial Monoids

by

J. A. Brzozowski and Faith E. Fich

Abstract

We consider the family of languages whose syntactic monoids are $\mathcal{R}$-trivial. Languages whose syntactic monoids are $\mathcal{J}$-trivial correspond to a congruence which tests the subwords of length n or less that appear in a given word, for some integer n. We show that in the $\mathcal{R}$-trivial case the required congruence also takes into account the order in which these subwords first appear, from left to right. Characterizations of the related finite automata and regular expressions are summarized. Dual results for $\mathcal{L}$-trivial monoids are also discussed.

1. Introduction

The well-known Green equivalence relations are fundamental in the theory of monoids [2, 6]. They are defined as follows. Let M be a monoid and $f,g \in M$; then

$$\begin{aligned} f\mathcal{J}g &\text{ iff } MfM = MgM \\ f\mathcal{L}g &\text{ iff } Mf = Mg \\ f\mathcal{R}g &\text{ iff } fM = gM \\ f\mathcal{H}g &\text{ iff } f\mathcal{L}g \text{ and } f\mathcal{R}g \ . \end{aligned}$$

If ρ is an equivalence relation on M , we say that M is ρ-trivial iff $f\rho g$ implies $f = g$. In 1965 Schützenberger [8] showed that finite $\mathcal{H}$-trivial monoids correspond to star-free languages, i.e. languages that can be denoted by regular expressions using only boolean operations and concatenation. In 1972 Simon [9,10] characterized the languages corresponding to finite $\mathcal{J}$-trivial monoids. These languages play a key role in the dot-depth hierarchy [3, 9] of star-free languages. This hierarchy and $\mathcal{J}$-trivial and $\mathcal{H}$-trivial monoids are also treated in [4].

The languages corresponding to finite $\mathcal{R}$-trivial (and $\mathcal{L}$-trivial) monoids are studied here. Several new characterizations of these languages are given.

2. Terminology and Notation

Let A be a finite non-empty alphabet and A^* the free monoid generated by A , with unit element 1 (the empty word). The length of $x \in A^*$ is denoted by $|x|$; note that $|1| = 0$. The product (concatenation) of two words x and y in A^* is denoted by

xy . The "alphabet" of a word $x \in A^*$ is

$$\alpha(x) = \{a \in A \mid x = uav \text{ for some } u,v \in A^*\} .$$

The reverse x^ρ of a word x is defined by induction on $|x|$:

$$1^\rho = 1 \quad \text{and} \quad (xa)^\rho = ax^\rho .$$

Subsets of A^* are called languages. If $X,Y \subseteq A^*$ then $\overline{X} = A^* - X$, $X \cup Y$, and $X \cap Y$ denote the complement of X , the union, and intersection of X and Y , respectively. The product of two languages is $XY = \{w \mid w = xy , x \in X , y \in Y\}$. Also $X^* = \bigcup_{n\geq 0} X^n$ (where $X^0 = \{1\}$) is the submonoid of A^* generated by X . The reverse of X is $X^\rho = \{x^\rho \mid x \in X\}$.

For any family F of languages $F\underline{B}$ is the smallest family containing F and closed under complementation and finite unions. Similarly $F\underline{M}$ is the smallest family containing $F \cup \{\{1\}\}$ and closed under concatenation. Thus $F\underline{B}$ and $F\underline{M}$ are the boolean algebra and monoid generated by F , respectively.

The syntactic congruence $\equiv_X$ of $X \subseteq A^*$ is defined as follows. For all $u,v,x,y \in A^*$

$$x \equiv_X y \text{ iff } (uxv \in X \text{ iff } uyv \in X) .$$

The quotient monoid $M = A^*/\equiv_X$ is the syntactic monoid of X and the natural morphism $\varphi : A^* \to M$, mapping $x \in A^*$ onto the equivalence class of $\equiv_X$ containing x , is the syntactic morphism of X . For convenience we often denote $\varphi(x)$ by $\underline{x}$.

If $\sim$ is any congruence on A^* we say that X is a $\sim$ language iff X is a union of congruence classes of $\sim$. Thus X

is a $\sim$ language iff for all $x,y \in A^*$

$$x \sim y \text{ implies } (x \in X \text{ iff } y \in X) \text{ .}$$

Since $\sim$ is a congruence, $x \sim y$ implies $uxv \sim uyv$ for all $u,v \in A^*$. Thus X is a $\sim$ language iff

$$x \sim y \text{ implies } x \equiv_X y \text{ , i.e. } \underline{x} = \underline{y} \text{ .}$$

A finite semiautomaton is a triple $\underset{\sim}{S} = \langle A, Q, \sigma\rangle$, where A is the input alphabet, Q is a finite set of states and $\sigma : Q \times A \to Q$ is the transition function. A finite automaton is a system $\underset{\sim}{A} = \langle A, Q, q_0, F, \sigma\rangle$ where A, Q and σ are as above, $q_0 \in Q$ is the initial state, and $F \subseteq Q$ is the set of final states. In any finite semiautomaton define the relation $\to$ as follows. For $p,q \in Q$

$$p \to q \text{ iff } \sigma(p, x) = q$$

for some $x \in A^*$. $\underset{\sim}{S}$ (or $\underset{\sim}{A}$) is partially ordered iff the relation $\to$ on Q is a partial order. A semiautomaton is a chain reset iff $\to$ is a total order.

The direct product of two semiautomata $\underset{\sim}{S} = \langle A, Q, \sigma\rangle$ and $\underset{\sim}{T} = \langle A, P, \tau\rangle$ is the semiautomaton $\underset{\sim}{S} \times \underset{\sim}{T} = \langle A, Q{\times}P, \pi\rangle$, where

$$\pi((q, p), a) = (\sigma(q, a), \tau(p, a)) \text{ .}$$

The cascade product of $\underset{\sim}{S} = \langle A, Q, \sigma\rangle$ and $\underset{\sim}{T} = \langle B, P, \tau\rangle$ with connection $\omega : Q \times A \to B$ is the semiautomaton $\underset{\sim}{S} \circ \underset{\sim}{T} = \langle A, Q{\times}P, \pi\rangle$, where

$$\pi((q, p), a) = (\sigma(q, a), \tau(p, \omega(q, a)) \text{ .}$$

An initialized semiautomaton is a semiautomaton with an initial state, i.e. $\underset{\sim}{S} = \langle A, Q, q_0, \sigma\rangle$. Let $\underset{\sim}{S}$ and $\underset{\sim}{T} = \langle B, P, p_0, \tau\rangle$ be two initialized semiautomata. $\underset{\sim}{T}$ is a subsemiautomaton of $\underset{\sim}{S}$ iff $B \subseteq A$, $P \subseteq Q$, $q_0 = p_0$, and τ is the restriction of σ to $P \times B$. A semiautomaton $\underset{\sim}{S}$ is a homomorphic image of semiautomaton $\underset{\sim}{T}$ iff $B = A$ and there exists a surjective mapping $\psi : P \to Q$ such that $\psi(p_0) = q_0$ and

$$\psi(\tau(p, a)) = \sigma(\psi(p), a) \quad .$$

$\underset{\sim}{S}$ is covered by $\underset{\sim}{T}$ iff $\underset{\sim}{S}$ is a homomorphic image of a subsemiautomaton of $\underset{\sim}{T}$.

The transformation monoid of a semiautomaton $\underset{\sim}{S} = \langle A, Q, \sigma \rangle$ (or of a finite automaton $\langle A, Q, q_0, F, \sigma \rangle$) is the set of all transformations of Q onto itself of the form $(q_1, \ldots, q_n) \to (\sigma(q_1, x), \ldots, \sigma(q_n, x))$ for some $x \in A^*$. It is well-known that if $\underset{\sim}{A}$ is a reduced finite automaton recognizing the language $X \subseteq A^*$, then the transformation monoid of $\underset{\sim}{A}$ is isomorphic to the syntactic monoid of X.

Let M be any monoid and $f \in M$. Then $P_f = \{g \in M \mid f \in MgM\}$ and $M_f = P_f^*$. Thus M_f is the submonoid of M generated by the elements g "with which f can be written" $(f \in MgM)$.

3. Languages of $\mathcal{J}$-Trivial Monoids

Simon, in [9] and [10], provides many characterizations for languages with $\mathcal{J}$-trivial syntactic monoids as is summarized in the following theorem. An additional property, M3 , is taken from [1].

Theorem 1 Let $X \subseteq A^*$ be a regular language, let M be its syntactic monoid, and let $\underset{\sim}{A}$ and $\underset{\sim}{A}^{\rho}$ be the reduced finite automata accepting X and X^{ρ} respectively. The following conditions are equivalent.

M1. M is $\mathcal{J}$-trivial

M2. M is $\mathcal{R}$-trivial and $\mathcal{L}$-trivial

M3. For all idempotents $e \in M$, $eM_e \cup M_e e = e$.

M4. There exists an $n > 0$ such that for all $f,g \in M$, $(fg)^n = (fg)^n f = g(fg)^n$.

M5. There exists an $n > 0$ such that for all $f,g \in M$ $f^n = f^{n+1}$ and $(fg)^n = (gf)^n$.

X1. X is a ${}_n\!\sim$ language for some $n \geq 0$.

E1. $X \in \{A^*aA^* \mid a \in A\}\underline{MB}$

A1. $\underset{\sim}{A}$ and $\underset{\sim}{A}^{\rho}$ are both partially ordered.

A2. $\underset{\sim}{A}$ is partially ordered and for all $q \in Q$, $x,y \in A^*$ $\tau(q,x) = \tau(q,xx) = \tau(q,xy)$ and $\tau(q,y) = \tau(q,yy) = \tau(q,yx)$ imply $\tau(q,x) = \tau(q,y)$.

A3. $\underset{\sim}{A}$ can be covered by a direct product of chain resets.

This paper provides analogous results for languages with $\mathcal{R}$-trivial syntactic monoids. We require the following concepts from [9].

The congruence ${}_n{\sim}$, mentioned above, is defined in terms of the subwords of length less than or equal to n that a given word contains. More precisely we have:

<u>Definition 2</u> Let $x,y \in A^*$ and $n \geq 0$. Then

(a) x is a <u>subword</u> of y , $x \leq y$, if and only if there exist $x_1,\ldots,x_n,u_0,\ldots,u_n \in A^*$ such that $x = x_1\ldots x_n$ and $y = u_0x_1u_1\ldots x_nu_n$

(b) the <u>n-contents</u> of y , denoted by $\mu_n(y)$, is the set $\{x \mid x \leq y \text{ and } |x| \leq n\}$

(c) $x \;{}_n{\sim}\; y$ iff $\mu_n(x) = \mu_n(y)$

It is straightforward to show that ${}_n{\sim}$ is a congruence of finite index for any $n \geq 0$ [9]. Simon also proves the following three results which are needed for the next section.

<u>Proposition 3</u> Let $x,y \in A^*$ and $n \geq 0$. Then

(a) $x^n \;{}_n{\sim}\; x^{n+1}$

(b) $(xy)^n \;{}_n{\sim}\; (xy)^nx$

(c) $(xy)^n \;{}_n{\sim}\; y(xy)^n$.

<u>Proposition 4</u> Let $x,y \in A^*$ and $n \geq 0$. Then $x \;{}_{n+1}{\sim}\; y$ implies $x \;{}_n{\sim}\; y$.

<u>Lemma 5</u> Let $u,v \in A^*$ and $n > 0$. Then $u \;{}_n{\sim}\; uv$ iff there exist $u_1,\ldots,u_n \in A^*$ such that $u = u_1\ldots u_n$ and

$\alpha(u_1) \supseteq \alpha(u_2) \supseteq \ldots \supseteq \alpha(u_n) \supseteq \alpha(v)$.

4. The ${}_n{\sim}_R$ Congruence

The congruence ${}_n{\sim}_R$ is defined to be a refinement of ${}_n{\sim}$ in which the order of appearance(from the left)of the subwords in a word is also taken into account. More formally:

Definition 6 Let $x,y \in A^*$ and $n \geq 0$. Then $x \; {}_n{\sim}_R \; y$ if and only if

(a) for each prefix u of x there exists a prefix v of y such that $u \; {}_n{\sim} \; v$,

and (b) for each prefix v of y there exists a prefix u of x such that $u \; {}_n{\sim} \; v$.

Note that if $|x| < n$, $x \; {}_n{\sim}_R \; y$ iff $x = y$.

The two equivalence relations ${}_n{\sim}$ and ${}_n{\sim}_R$ are closely related and satisfy many similar properties.

Proposition 7 Let $x,y \in A^*$ and $n \geq 0$.

(a) If $x \; {}_n{\sim}_R \; y$ then $x \; {}_n{\sim} \; y$.

(b) $x \; {}_n{\sim} \; xy$ if and only if $x \; {}_n{\sim}_R \; xy$.

(c) If $xy \; {}_n{\sim}_R \; x'y'$ and $x \; {}_n{\sim} \; x'$ then $x \; {}_n{\sim}_R \; x'$.

Proof:

(a) Since x is a prefix of x there exists a prefix v of y such that $x \; {}_n{\sim} \; v$. Thus $\mu_n(x) = \mu_n(v) \subseteq \mu_n(y)$. Similarly $\mu_n(y) \subseteq \mu_n(x)$; so $\mu_n(x) = \mu_n(y)$. Therefore $x \; {}_n{\sim} \; y$.

(b) Any prefix of x is also a prefix of xy. Let v be any prefix of xy. Then either v is a prefix of x or x is a prefix of v. In the second case $\mu_n(x) \subseteq \mu_n(v) \subseteq \mu_n(xy) = \mu_n(x)$ so that $x \ {}_n\!\sim v$. Therefore $x \ {}_n\!\sim_R xy$. The converse follows from (a).

(c) Let u be a prefix of x. Since u is also a prefix of xy there exists a prefix u' of $x'y'$ such that $u \ {}_n\!\sim u'$. Now either u' is a prefix of x' or x' is a prefix of u'. In the second case $\mu_n(x') \subseteq \mu_n(u') = \mu_n(u) \subseteq \mu_n(x) = \mu_n(x')$, so that $x' \ {}_n\!\sim u'$ and hence $u \ {}_n\!\sim x'$. Similarly for each prefix u' of x' there exists a prefix u of x such that $u \ {}_n\!\sim u'$. Therefore $x \ {}_n\!\sim_R x'$.

<u>Proposition 8</u> Let $x,y \in A^*$ and $n \geq 0$. Then

(a) $x^n \ {}_n\!\sim_R x^{n+1}$

(b) $(xy)^n \ {}_n\!\sim_R (xy)^n x$.

<u>Proof:</u> Immediate from Propositions 3 (a) and (b) and 7 (b).

<u>Proposition 9</u> Let $x,y \in A^*$ and $n \geq 0$. Then $x \ {}_{n+1}\!\sim_R y$ implies $x \ {}_n\!\sim_R y$.

<u>Proof:</u> Follows from Proposition 4.

<u>Lemma 10</u> Let $u,v \in A^*$ and $n > 0$. Then $u \ {}_n\!\sim_R uv$ iff there exist $u_1,\ldots,u_n \in A^*$ such that $u = u_1\ldots u_n$ and $\alpha(u_1) \supseteq \ldots \supseteq \alpha(u_n) \supseteq \alpha(v)$.

<u>Proof:</u> Follows from Lemma 5 and Proposition 7.

<u>Proposition 11</u> ${}_n\sim_R$ is a congruence of finite index for all $n \geq 0$.

<u>Proof:</u> Let $n \geq 0$ and let $x,y \in A^*$ be such that $x \; {}_n\sim_R \; y$. Let $a \in A$.

Suppose u is a prefix of xa . Then either u is a prefix of x or $u = xa$. In the first case, because $x \; {}_n\sim_R \; y$, there is a prefix v of y such that $u \; {}_n\sim \; v$. If $u = xa$ then from Proposition 7(a) $x \; {}_n\sim \; y$, and since ${}_n\sim$ is a congruence $u = xa \; {}_n\sim \; ya$. By symmetry, for each prefix v of ya there exists a prefix u of xa such that $u \; {}_n\sim \; v$. Therefore ${}_n\sim_R$ is a right congruence.

Suppose u is a prefix of ax . Then either $u = 1$ or $u = au'$ for some prefix u' of x . If $u = 1$ then u is also a prefix of ay . Otherwise, since $x \; {}_n\sim_R \; y$, there exists a prefix v' of y such that $u' \; {}_n\sim \; v'$. But ${}_n\sim$ is a congruence so $u = au' \; {}_n\sim \; av'$. Similarly for each prefix v of ay there exists a prefix u of ax such that $u \; {}_n\sim \; v$. Hence ${}_n\sim_R$ is a left congruence.

The fact that ${}_n\sim_R$ is of finite index follows directly from the fact that ${}_n\sim$ is of finite index.

One nice property of ${}_n\sim_R$, which is not shared by ${}_n\sim$, is that each congruence class has a unique shortest element.

<u>Lemma 12</u> Every congruence class of ${}_n\sim_R$ contains a unique element of minimal length. Furthermore, if $a_1,\ldots,a_m \in A$ then $a_1 \ldots a_m$ is minimal if and only if $\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \mu_n(a_1 a_2) \subsetneq \ldots \subsetneq \mu_n(a_1 \ldots a_m)$.

<u>Proof:</u> By induction on k, the minimum length of elements in a given ${}_n{\sim}_R$ class.

Note that minimum length elements exist because length is a function from A^* to the nonnegative integers which form a well ordered set.

For $k = 0$ the lemma is true since 1 is the only word of length 0. Let $k \geq 1$ and assume the lemma is true for all ${}_n{\sim}_R$ classes containing elements of length less than k.

Suppose there exists a ${}_n{\sim}_R$ class containing minimal elements x and y of length k.

Since $k \geq 1$, $x = ua$ for some $u \in A^*$, $a \in A$. Now $\mu_n(u) \subseteq \mu_n(x)$, and $u \; {}_n{\sim} \; x$ implies $u \; {}_n{\sim}_R \; x$ by Proposition 7(b), so $\mu_n(u) \neq \mu_n(x)$. Employing the induction hypothesis (since $|u| < k$) the ${}_n{\sim}_R$ class containing u has a unique element of minimal length. Call this element w. If $w \neq u$ then $|w| < |u|$ and hence $|wa| < |x|$. But $w \; {}_n{\sim}_R \; u$ and ${}_n{\sim}_R$ is a congruence, so $wa \; {}_n{\sim}_R \; ua = x$ contradicting the minimality of x. Therefore $u = w$. By the induction hypothesis $u = a_1 \ldots a_m$ where $\mu_n(a_1) \subsetneq \ldots \subsetneq \mu_n(a_1 \ldots a_m)$ and thus $x = a_1 \ldots a_m a$ where $\mu_n(a_1) \subsetneq \ldots \subsetneq \mu_n(a_1 \ldots a_m) \subsetneq \mu_n(a_1 \ldots a_m a)$.

Because $x \; {}_n{\sim}_R \; y$ there exists a prefix v of y such that $u \; {}_n{\sim} \; v$. By Proposition 7(c) $u \; {}_n{\sim}_R \; v$. Also, v is a proper prefix of y since $\mu_n(v) = \mu_n(u) \subsetneq \mu_n(x) = \mu_n(y)$. Thus $v = u$, for otherwise $k = |y| \geq 1 + |v| > 1 + |u| = |x| = k$ which is impossible. Therefore $y = ua'$ for some $a' \in A$. Now $\mu_n(u) \subsetneq \mu_n(ua)$; hence there exists a word $za \in \mu_n(ua) - \mu_n(u)$. But $\mu_n(ua) = \mu_n(ua')$, so $za \in \mu_n(ua') - \mu_n(u)$. That being the case $a = a'$ and thus $x = y$.

By induction on k every congruence class of ${}_n{\sim}_R$ contains a unique element of minimal length, and if $a_1,\dots,a_m \in A$ are such that $a_1\dots a_m$ is minimal then $\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \dots \subsetneq \mu_n(a_1\dots a_m)$.

Finally, suppose $x = a_1\dots a_m$ where $a_1,\dots,a_m \in A$ and $\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \dots \subsetneq \mu_n(a_1\dots a_m)$. Let $u_0 = 1$, $u_1 = a_1$, ..., $u_m = a_1\dots a_m$ be the prefixes of x and let y be the unique minimal element of the ${}_n{\sim}_R$ class containing x . Since $x \; {}_n{\sim}_R \; y$ there exist prefixes v_0, v_1, ..., v_m of y such that $u_i \; {}_n{\sim} \; v_i$ for $0 \leq i \leq m$. Because $\mu_n(v_i) = \mu_n(u_i) \neq \mu_n(u_j) = \mu_n(v_j)$ for all $i \neq j$, the v_i's must be distinct. Thus $|y| \geq m$. But $|x| = m$; therefore by the uniqueness of the minimal element $x = y$.

Definition 13 For $n \geq 0$ define the function $\chi_n : A^* \to A^*$ by $\chi_n(x)$ = the unique minimal element ${}_n{\sim}_R$ congruent to x .

The following is an algorithm for finding the minimal element of a congruence class of ${}_n{\sim}_R$ given any word x in the class.

Algorithm for $\chi_n(x)$

Find the shortest prefix ua of x such that $u \in A^*$, $a \in A$, and $u \; {}_n{\sim} \; ua$. If none exists then $x = a_1\dots a_m$ where

$$\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \mu_n(a_1a_2) \subsetneq \dots \subsetneq \mu_n(a_1\dots a_m) \quad \text{and} \quad \chi_n(x) = x \ .$$

Otherwise $x = uav$ for some $v \in A^*$. Since $u \; {}_n{\sim} \; ua$ implies $u \; {}_n{\sim}_R \; ua$ and ${}_n{\sim}_R$ is a congruence, $uv \; {}_n{\sim}_R \; uav = x$. Thus $\chi_n(x) = \chi_n(uv)$. Note that uv is shorter than x and so the algorithm always terminates.

<u>Example</u> Let $x = abccbcac$ and $n = 2$

prefix u of x	$\mu_2(u)$
1	1
a	1,a
ab	1,a,b,ab
abc	1,a,b,ab,c,ac,bc
abcc	1,a,b,ab,c,ac,bc,cc
abccb	1,a,b,ab,c,ac,bc,cc,cb,bb
abccbc	1,a,b,ab,c,ac,bc,cc,cb,bb

Since $\mu_2(abccb) = \mu_2(abccbc)$, $abccb \;{}_{2}{\sim}_{R}\; abccbc$ and hence $abccbac \;{}_{2}{\sim}_{R}\; abccbcac = x$. Replace x by $abccbac$.

abccba	1,a,b,ab,c,ac,bc,cc,cb,bb,aa,ba,ca
abccbac	1,a,b,ab,c,ac,bc,cc,cb,bb,aa,ba,ca

Since $\mu_2(abccba) = \mu_2(abccbac)$, $abccba \;{}_{2}{\sim}_{R}\; abccbac$. Now $\mu_2(1) \subsetneq \mu_2(a) \subsetneq \mu_2(ab) \subsetneq \mu_2(abc) \subsetneq \mu_2(abcc) \subsetneq \mu_2(abccb) \subsetneq \mu_2(abccba)$; therefore $\chi_2(x) = abccba$.

To construct $\mu_n(ua)$ from $\mu_n(u)$ it is only necessary to add those elements wa such that $w \in \mu_{n-1}(u)$ but $wa \notin \mu_n(u)$. The number of elements in $\mu_n(u)$ is bounded by $\sum_{i=0}^{n} m^i$, where m is the cardinality of the alphabet. Given x , $\chi_n(x)$ can be found in $O(|x|)$ steps. Thus in $O(|x| + |y|)$ steps one can determine whether $x \;{}_{n}{\sim}_{R}\; y$.

The algorithm motivates the following definition:

<u>Definition 14</u> For $n \geq 0$ define the binary relation ${}_{n}\dot{\simeq}_{R}$ on A^* as follows:

$$x \ {}_{n}\dot{\simeq}_{R} \ y \quad \text{iff} \quad x = z_1 u z_2 \quad \text{and} \quad y = z_1 u v z_2 \quad \text{for some}$$
$$z_1, z_2, u, v \in A^* \quad \text{such that} \quad u \ {}_{n}\sim \ uv .$$

Let ${}_{n}\simeq_{R}$ be the symmetric transitive closure of ${}_{n}\dot{\simeq}_{R}$.

One verifies that $x \ {}_{n}\dot{\simeq}_{R} \ x$ for all $x \in A^*$ since $1^n = 1 \ {}_{n}\sim \ 1 = 1^n 1$, $x = x(1^n)1$ and $x = x(1^n 1)1$. Hence ${}_{n}\simeq_{R}$ is an equivalence relation over A^* . It is easily seen to be a congruence.

<u>Propositions 15</u> Let $n \geq 0$. Then $x \ {}_{n}\simeq_{R} \ y$ iff $x \ {}_{n}\simeq_{R} \ y$.

<u>Proof</u>: If $x \ {}_{n}\dot{\simeq}_{R} \ y$ then $x \ {}_{n}\sim_{R} \ y$ by Proposition 7(b); thus $x \ {}_{n}\simeq_{R} \ y$ implies $x \ {}_{n}\sim_{R} \ y$ since ${}_{n}\sim_{R}$ is transitive.

If $x \ {}_{n}\sim_{R} \ y$ then by Lemma 12, $\chi_n(x) = \chi_n(x)$. From the algorithm it follows that $x \ {}_{n}\simeq_{R} \ \chi_n(x)$ and $y \ {}_{n}\simeq_{R} \ \chi_n(y)$. Hence $x \ {}_{n}\simeq_{R} \ y$.

5. <u>*R*-trivial Monoids</u>

The following theorem is from [8] and [1].

<u>Theorem 16</u> Let M be a finite monoid. The following conditions are equivalent.

1. M is *R*-trivial.
2. For all $f,g,h \in M$, $fgh = f$ implies $fg = f$.
3. For all idempotents $e \in M$, $eM_e = e$.
4. There exists $n > 0$ such that, for all $f,g \in M$, $(fg)^n f = (fg)^n$.

<u>Lemma 17</u> Let M be a finite R-trivial monoid and $\varphi : A^* \to M$ a surjective morphism. Let n be the cardinality of M and let $u,v \in A^*$. Then

$$u \;{}_n\!\sim uv \quad \text{implies} \quad \underline{u} = \underline{uv} \ ,$$

where $\underline{x}$ denotes $\varphi(x)$.

<u>Proof:</u> Suppose $u \;{}_n\!\sim uv$. By Lemma 5, there exist $u_1,\dots,u_n \in A^*$ such that $u = u_1 \dots u_n$ and $\alpha(u_1) \supseteq \dots \supseteq \alpha(u_n) \supseteq \alpha(v)$. Let $u_o = 1$. By the choice of n , the elements $\underline{u}_o$, $\underline{u}_o\underline{u}_1$, ..., $\underline{u}_o\underline{u}_1\dots\underline{u}_n$, cannot all be distinct. Hence there exist i and j , $0 \le i < j \le n$, such that

$$f = \underline{u}_o \dots \underline{u}_i = \underline{u}_o \dots \underline{u}_i \dots \underline{u}_j = f\underline{u}_{i+1} \dots \underline{u}_j = f\underline{u}_{i+1}(\underline{u}_{i+2} \dots \underline{u}_j) \ .$$

Since M is R-trivial, $f = f\underline{u}_{i+1}$. If $\alpha(u_n) = \phi$ then $v = 1$ and there is nothing to prove. Thus suppose $\alpha(u_n) \neq \phi$. Since $\alpha(u_{i+1}) \supseteq \alpha(u_n) \neq \phi$, we have $u_{i+1} = az$ for some $a \in \alpha(u_{i+1})$, $z \in A^*$. Then $f = f\underline{az}$ and $f = f\underline{a}$. Consequently $f = f\underline{a}$ for all $a \in \alpha(u_{i+1})$. Because $u_{i+1} \dots u_n v \in (\alpha(u_{i+1}))^*$ it follows that

$$\underline{u} = \underline{u}_o \dots \underline{u}_n = f\underline{u}_{i+1} \dots \underline{u}_n = f\underline{u}_{i+1} \dots \underline{u}_n \underline{v} = \underline{uv} \ .$$

<u>Theorem 18</u> Let M be the syntactic monoid of $X \subseteq A^*$. Then M is finite and R-trivial if and only if X is a ${}_n\!\sim_R$ language for some $n \ge 0$.

<u>Proof:</u> Assume M is finite and R-trivial. Let n be the cardinality of M and let $x,y \in A^*$. Suppose $x \;{}_n\!\dot{\simeq}_R\; y$. Then $x = z_1 u z_2$ and $y = z_1 uv z_2$ for some $z_1, z_2, u, v \in A^*$ such that $u \;{}_n\!\sim uv$. By Lemma 17, $\underline{u} = \underline{uv}$ and $\underline{x} = \underline{z}_1\underline{uz}_2 = \underline{z}_1\underline{uvz}_2 = \underline{y}$. Since ${}_n\!\simeq_R$ is the

symmetric transitive closure of ${}_{n}\dot{\simeq}_{R}$, it follows that $x \;{}_{n}\simeq_{R}\; y$ implies $\underline{x} = \underline{y}$. By Proposition 15 $x \;{}_{n}\sim_{R}\; y$ iff $x \;{}_{n}\simeq_{R}\; y$. Thus $x \;{}_{n}\sim_{R}\; y$ implies $\underline{x} = \underline{y}$ i.e. X is a ${}_{n}\sim_{R}$ language.

By Proposition 8, for all $x,y \in A^*$,

$$(xy)^n \;{}_{n}\sim_{R}\; (xy)^n x \quad .$$

If X is a ${}_{n}\sim_{R}$ language we must have

$$(\underline{xy})^n = (\underline{xy})^n \underline{x} \ .$$

Since M is the range of the surjective morphism $\varphi : A^* \to M$, it follows that for all $f,g \in M$,

$$(fg)^n = (fg)^n f \quad .$$

Because ${}_{n}\sim_{R}$ is of finite index M is finite, and it is $\mathcal{R}$-trivial by Theorem 16.

6. Partially Ordered Finite Automata

In this section the finite automata associated with ${}_{n}\sim_{R}$ languages are considered. In the sequel we assume that all semiautomata and automata are finite.

Recall the definition of partially ordered automata and semiautomata given in the introduction. The following equivalent characterization is from [9].

Proposition 19 $\underset{\sim}{S} = \langle A, Q, \sigma \rangle$ is partially ordered if and only if for all $q \in Q$, $x,y \in A^*$, $\sigma(q, xy) = q$ implies $\sigma(q, x) = q$.

Proposition 20   Let $\underset{\sim}{S} = \langle A, Q, \sigma\rangle$ be a partially ordered semi-automaton. Then the transformation monoid, M, of $\underset{\sim}{S}$ is $\mathcal{R}$-trivial.

Proof: Suppose $f,g,h \in M$ are such that $fgh = f$. Since M is the transformation monoid of $\underset{\sim}{S}$ there exist $x,y,z \in A^*$ such that $\underline{x} = f$, $\underline{y} = g$, and $\underline{z} = h$. Now $\underline{xyz} = fgh = f = \underline{x}$ and $\underset{\sim}{S}$ is partially ordered. Thus $\sigma(q, x) = \sigma(q, xyz) = \sigma(\sigma(q, x), yz)$,and by Proposition 19, $\sigma(q, x) = \sigma(\sigma(q, x), y) = \sigma(q, xy)$ for all $q \in Q$. Therefore $f = \underline{x} = \underline{xy} = fg$.

We now present additional properties of partially ordered semiautomata mentioned in [7], [9], and [11]. The proofs of these results are straightforward and can be easily verified by the reader.

Proposition 21   If $\underset{\sim}{T}$ is a semiautomaton which is covered by some partially ordered semiautomaton $\underset{\sim}{S}$ then $\underset{\sim}{T}$ is partially ordered.

Proposition 22   The direct product of two partially ordered semiautomata is partially ordered.

Proposition 23   The cascade product of two partially ordered semiautomata is partially ordered.

Let $\underset{\sim}{A} = \langle A, Q, q_0, F, \sigma\rangle$ and $\underset{\sim}{B} = \langle A, P, p_0, G, \tau\rangle$ be finite automata and let $\langle A, Q\times P, \pi\rangle = \langle A, Q, \sigma\rangle \times \langle A, P, \tau\rangle$. Then the union of $\underset{\sim}{A}$ and $\underset{\sim}{B}$ is

$$\underset{\sim}{A} \cup \underset{\sim}{B} = \langle A, Q\times P, (q_0, p_0), F\times P\cup Q\times G, \pi\rangle \quad ,$$

the intersection of $\underset{\sim}{A}$ and $\underset{\sim}{B}$ is

$$\underset{\sim}{A} \cap \underset{\sim}{B} = \langle A,\ Q{\times}P,\ (q_o,\ p_o),\ F{\times}G,\ \pi\rangle \quad ,$$

and the complement of $\underset{\sim}{A}$ is

$$\bar{\underset{\sim}{A}} = \langle A,\ Q,\ q_o,\ Q\text{-}F,\ \sigma\rangle \ .$$

Because the definition of a partially ordered automaton does not depend on the set of final states it follows that if $\underset{\sim}{A}$ and $\underset{\sim}{B}$ are partially ordered then $\underset{\sim}{A} \cup \underset{\sim}{B}$, $\underset{\sim}{A} \cap \underset{\sim}{B}$, and $\bar{\underset{\sim}{A}}$ are also. Hence the set of all partially ordered finite automata with alphabet A forms a Boolean algebra.

Another way partially ordered automata can be characterized is in terms of certain sequential networks.

Definition 24 For $n \geq 0$, an *n-way fork* is an initialized semi-automaton $\langle A,\ \{q_o, q_1, \ldots, q_n\},\ q_o,\ \sigma\rangle$ where $A = A_o \cup A_1 \cup \ldots \cup A_n$, the A_i's are non-empty and pairwise disjoint, $\sigma(q_o,\ a) = q_i$ for all $a \in A_i$, and $\sigma(q_i,\ a) = q_i$ for all $a \in A$, $i = 1,\ldots,n$. See Fig. 1. A *half-reset* is a one-way fork.

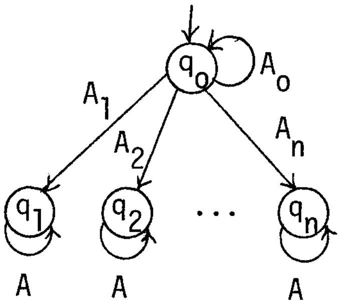

Fig. 1 An n-way fork

Proposition 25 If a semiautomaton can be covered by a cascade product of half-resets then it is partially ordered.

Proof: Immediate from Propositions 21 and 23 and the fact that a half-reset is partially ordered.

In [7] and [11] it is proved that any partially ordered finite automaton can be covered by a cascade product of half-resets. Introducing n-way forks is a convenient intermediate step.

Proposition 26 Any n-way fork is isomorphic to the connected initialized subsemiautomaton of a cascade product of n half-resets.

Proof: By induction on n. The case $n = 0$ is degenerate. For $n = 1$ the result follows from the definition of a half-reset. Assume the result is true for $n \geq 1$. Consider the (n+1)-way fork $\underset{\sim}{F}_{n+1}$ illustrated in Fig. 2(a).

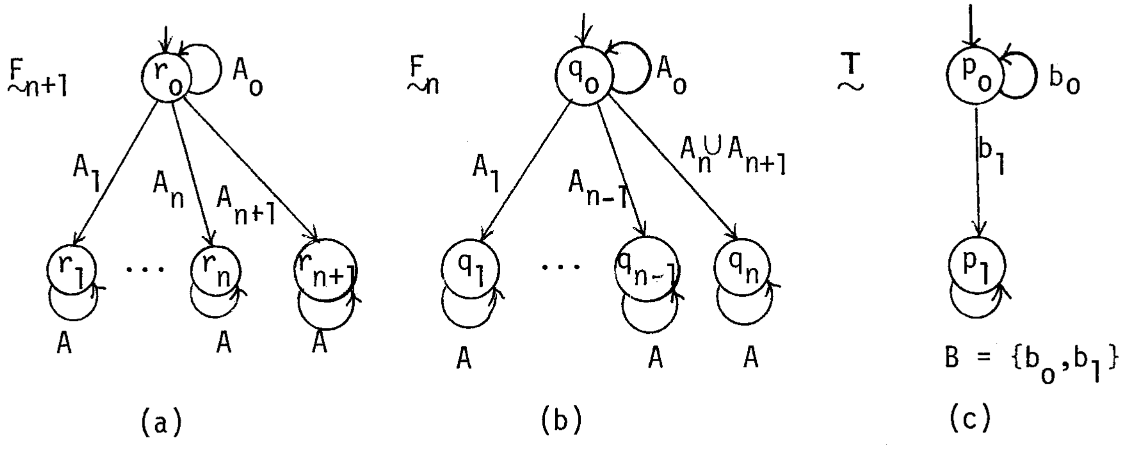

Fig. 2

Let $\underset{\sim}{F}_n$ = <A, Q, q_0, σ> be the n-way fork of Fig. 2(b) and let $\underset{\sim}{T}$ = <{b_0,b_1}, P, p_0, τ> be the half-reset in Fig. 2(c). Define the connection ω as follows:

$$\omega(q, a) = \begin{cases} b_1 & \text{if } q = q_0 \text{ and } a \in A_{n+1} \\ b_0 & \text{otherwise} \end{cases}$$

Let $\underset{\sim}{R}$ = <A, R, (q_0,p_0), η> be the connected initialized subsemiautomaton of $\underset{\sim}{F}_n \circ \underset{\sim}{T}$. Note that $R = \{(q_0,p_0), (q_1,p_0), \ldots, (q_n,p_0),(q_n,p_1)\}$ since these are the only states which are accessible from (q_0,p_0) . Except for (q_0,p_0) each is a terminal state (i.e. $\eta(r, a) = r$ for all $a \in A$, $r \in R - \{(p_0,q_0)\}$). It is clear that $\underset{\sim}{F}_{n+1}$ is isomorphic to $\underset{\sim}{R}$.

By the induction hypothesis $\underset{\sim}{F}_n$ is isomorphic to the connected initialized subsemiautomaton of a cascade product of n half-resets; therefore $\underset{\sim}{F}_{n+1}$ is isomorphic to the connected initialized subsemiautomaton of a cascade product of n+1 half-resets. Thus the result is true for all $n \geq 1$.

We call a graph G <u>tree-like</u> if and only if the graph G', obtained from G by removing all trivial loops, is a tree. (A trivial loop is an edge from a vertex to itself.) The height of G is defined to be the height of the tree G' .

<u>Proposition 27</u> Any initialized semiautomaton whose state graph is tree-like is isomorphic to the connected initialized subsemiautomaton of a cascade product of forks.

<u>Proof</u>: By induction on the height of the graph.

If the graph of an initialized semiautomaton is tree-like of height less than or equal to 1 then the semiautomaton is a fork. Assume the result is true for all initialized semiautomata whose graphs are tree-like of height less than h, where $h > 1$.

Let $\underset{\sim}{S} = \langle A, Q, q_0, \sigma \rangle$ be an initialized semiautomaton whose graph is tree-like of height h. Let $\{q_1,\dots,q_n\} = \{q \in Q - \{q_0\} \mid \sigma(q_0,a) = q$ for some $a \in A\}$ be the set of sons of q_0. For $1 \leq i \leq n$ let $\underset{\sim}{S}_i = \langle A, Q_i, q_i, \sigma_i \rangle$ be the sub-semiautomaton of $\underset{\sim}{S}$ initialized at q_i. Since $q_i \neq q_0$, the height of the graph is less than h; thus $\underset{\sim}{S}_i$ is isomorphic to the connected initialized subsemiautomaton of $\underset{\sim}{S}'_i = \langle A, Q'_i, q_i, \sigma'_i \rangle$, a cascade product of forks.

Define $\underset{\sim}{T}'_i = \langle B_i, Q'_i, q_i, \tau'_i \rangle$ as follows. If there exists an $a_i \in A$ such that $\sigma'_i(q, a_i) = q$ for all $q \in Q'_i$ let $B_i = A$ and $\tau'_i = \sigma'_i$. Otherwise let $B_i = A \cup \{e\}$, where $e \notin A$, and let τ'_i be such that for $q \in Q'_i$, $b \in B_i$,

$$\tau'_i(q, b) = \begin{cases} \sigma'_i(q, b) & \text{if } b \in A \\ q & \text{if } b = e \end{cases}.$$

Note that $\underset{\sim}{T}'_i$ is still a cascade product of forks.

Let $\underset{\sim}{T}_0 = \langle A, P, p_0, \tau_0 \rangle$ be the n-way fork where $P = \{p_0,p_1,\dots,p_n\}$ and

$$\tau_0(p, a) = \begin{cases} p_i & \text{if } p = p_0 \text{ and } \sigma(q_0,a) = q_i \\ p & \text{otherwise} \end{cases}$$

Inductively define $\underset{\sim}{T}_i = \underset{\sim}{T}_{i-1} \circ \underset{\sim}{T}'_i$ for $i = 1,\dots,n$ where the connection $\omega_i : P \times Q'_1 \times \dots \times Q'_{i-1} \times A \to B_i$ is given by

$$\omega_i(r, a) = \begin{cases} a & \text{if} \quad r = (p_i, q_1, \ldots, q_{i-1}) \\ b_i & \text{otherwise} \end{cases}$$

where $\tau_i'(q, b_i) = q$ for all $q \in Q_i'$.

It is a straightforward proof by induction to show that the set of states of $\underset{\sim}{T}_i$ accessible from the initial state $(p_o, q_1, \ldots, q_i)$ is

$$R_i = \{(p_o, q_1, \ldots, q_i)\} \cup \{(p_k, q_1, \ldots, q_{k-1}, q, q_{k+1}, \ldots, q_i) \\ \mid q \in Q_k', 1 \le k \le i\}$$

and that the following equations hold

$$\tau_i((p_o, q_1, \ldots, q_i), a) = (p_k, q_1, \ldots, q_i) \text{ for all } a \in A \text{ such that } \sigma(q_o, a) = q_k$$

$$\tau_i((p_k, q_1, \ldots, q_{k-1}, q, q_{k+1}, \ldots, q_i), a) \\ = (p_k, q_1, \ldots, q_{k-1}, \tau_k'(q, a), q_{k+1}, \ldots, q_i) \text{ for } q \in Q_k', 1 \le k \le i$$

and

$$\tau_i((p_k, q_1, \ldots, q_i), a) = (p_k, q_1, \ldots, q_i) \quad \text{for} \quad i < k \le n .$$

Now consider the bijection $\psi : Q \to R_n$ defined by

$$\psi(q) = \begin{cases} (p_o, q_1, \ldots, q_n) & \text{if} \quad q = q_o \\ (p_i, q_1, \ldots, q_{i-1}, \psi_i(q), q_{i+1}, \ldots, q_n) & \text{if} \quad q \in Q_i \end{cases}$$

where $\psi_i : Q_i \to Q_i'$ is the isomorphism from $\underset{\sim}{S}_i$ to the connected initialized subsemiautomaton of $\underset{\sim}{S}_i'$. Let $a \in A$ and $q \in Q$. If $q \in Q_i$ then

$$\begin{aligned}\psi(\sigma(q,\ a)) &= \psi(\sigma_i(q,\ a)) \\ &= (p_i,\ q_1,\ \ldots,\ q_{i-1},\ \psi_i(\sigma_i(q,\ a)),\ q_{i+1},\ \ldots,\ q_n) \\ &= (p_i,\ q_1,\ \ldots,\ q_{i-1},\ \sigma_i'(\psi_i(q),\ a),\ q_{i+1},\ \ldots,\ q_n) \\ &= (p_i,\ q_1,\ \ldots,\ q_{i-1},\ \tau_i'(\psi_i(q),\ a),\ q_{i+1},\ \ldots,\ q_n) \\ &= \tau_n((p_i,\ q_1,\ \ldots,\ q_{i-1},\ \psi_i(q),\ q_{i+1},\ q_n),\ a) \\ &= \tau_n(\psi(q),\ a)\end{aligned}$$

and if $q = q_0$ and $\sigma(q_0,\ a) = q_i$ then

$$\begin{aligned}\psi(\sigma(q,\ a)) &= \psi(q_i) \\ &= (p_i,\ q_1,\ \ldots,\ q_{i-1},\ \psi_i(q_i),\ q_{i+1},\ \ldots,\ q_n) \\ &= (p_i,\ q_1,\ \ldots,\ q_{i-1},\ q_i,\ q_{i+1},\ \ldots,\ q_n) \\ &= \tau_n((p_0,\ q_1,\ \ldots,\ q_n),\ a) \\ &= \tau_n(\psi(q_0),\ a)\quad .\end{aligned}$$

Thus ψ is an isomorphism between $\underset{\sim}{S}$ and the connected initialized subsemiautomaton of $\underset{\sim}{T}_n$; so the result is true for $\underset{\sim}{S}$. It follows by induction that the proposition is true.

<u>Corollary 28</u> Any partially ordered initialized semiautomaton is the homomorphic image of the connected initialized subsemiautomaton of a cascade product of half-resets.

<u>Proof</u>: Any partially ordered rooted graph can be transformed into a tree-like graph by splitting nodes (see Fig. 3). The desired homomorphism is the obvious one which maps a node in the tree-like graph to the node in the original graph from which it was produced. The result then follows by Proposition 27.

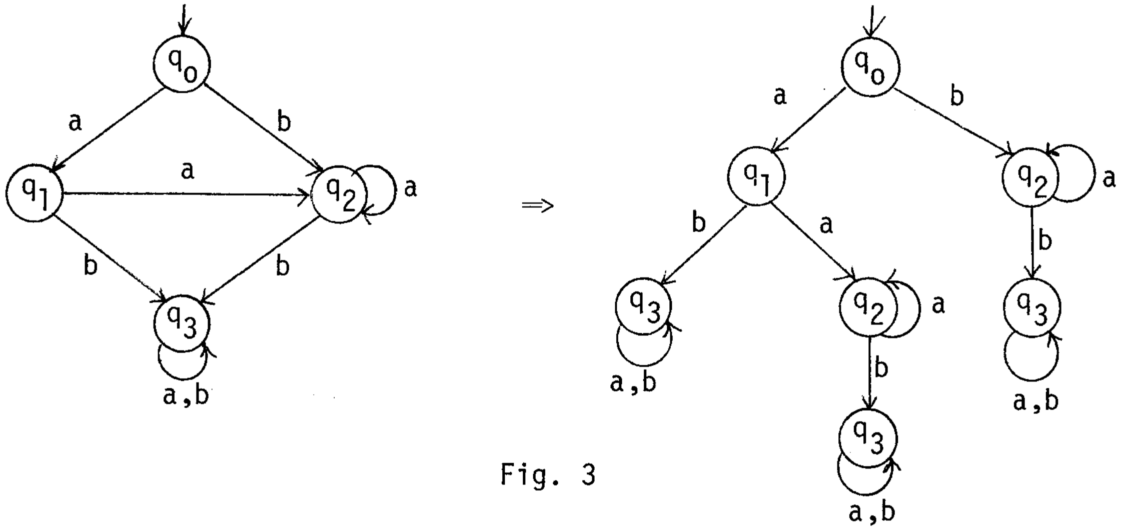

Fig. 3

7. $\mathcal{R}$-Expressions

Definition 29 Let A be a finite alphabet. An $\mathcal{R}$-expression is a finite union of regular expressions of the form $A_o^*a_1A_1^*\ldots a_mA_m^*$ where $m \geq 0$, $a_1,\ldots,a_m \in A$, and $A_{i-1} \subseteq A - \{a_i\}$ for $1 \leq i \leq m$.

The relationship between partially ordered semiautomata and $\mathcal{R}$-expressions is mentioned in [7].

Proposition 30 Let $X \subseteq A^*$ be the language denoted by some $\mathcal{R}$-expression. Then the reduced finite automaton recognizing X is partially ordered.

Proof: Because of the remark following Proposition 23 we may assume the expression is of the form $A_o^*a_1A_1^*\ldots a_mA_m^*$, where $m \geq 0$ and $A_{i-1} \subseteq A - \{a_i\}$ for $1 \leq i \leq m$, without any loss of generality.

Consider the automaton $\underset{\sim}{A} = \langle A, Q, q_o, \{q_n\}, \sigma\rangle$ where $Q = \{q_o, \ldots, q_n, q_d\}$ and σ is defined as follows:

$$\sigma(q_i, a) = \begin{cases} q_i & \text{if } a \in A_i \\ q_{i+1} & \text{if } a = a_{i+1} \\ q_d & \text{if } a \in A - (A_i \cup \{a_{i+1}\}) \end{cases}$$

$$\sigma(q_d, a) = q_d \quad \text{for all } a \in A \ .$$

It is straightforward to show that $\mathcal{A}$ is partially ordered and recognizes X .

Since the reduced finite automaton recognizing X is a homomorphic image of $\mathcal{A}$, it follows from Proposition 21 that it, too, is partially ordered.

<u>Proposition 31</u> Every ${}_n{\sim}_R$ language can be denoted by an $\mathcal{R}$-expression.

<u>Proof</u>: It is sufficient to show the result for every congruence class of ${}_n{\sim}_R$. The only ${}_o{\sim}_R$ class is the language denoted by A^* . Therefore assume $n > 0$. Let x be the minimal element of its congruence class. If $|x| = 0$ then, since $n > 0$, $\underline{x} = \underline{1} = \{1\}$ which can be denoted by ϕ^* . Otherwise $x = a_1 \ldots a_m$ for some $a_1, \ldots, a_m \in A$. Let $A_o = \phi$ and let $A_i = \{a \in A \mid a_1 \ldots a_i a \ {}_n{\sim} \ a_1 \ldots a_i\}$ for $1 \leq i \leq m$. Since x is minimal,

$$\mu_n(1) \subsetneq \mu_n(a_1) \subsetneq \cdots \subsetneq \mu_n(a_1 \ldots a_{i-1}) \subsetneq \mu_n(a_1 \ldots a_{i-1} a_i) \subsetneq \cdots \subsetneq \mu_n(a_1 \ldots a_m)$$

by Lemma 12. Hence $a_i \notin A_{i-1}$ for $1 \leq i \leq m$ and thus $A_o^* a_1 A_1^* \ldots a_m A_m^*$ is an $\mathcal{R}$-expression. From Proposition 15 it is clear that $\underline{x}$ can be denoted by $A_o^* a_1 A_1^* \ldots a_m A_m^*$.

With this result, Theorem 18, Proposition 20, and Proposition 30 the languages defined by the congruences $_n{\sim}_R$, $\mathcal{R}$-trivial monoids, partially ordered finite automata and $\mathcal{R}$-expressions are seen to be the same. Since the set of partially ordered finite automata over a given alphabet forms a Boolean algebra, the set of $\mathcal{R}$-expressions (over the same alphabet) also does. This result is used in the following theorem.

Proposition 32 Let A be an alphabet and let $\mathcal{D} = \{C^*a \mid C \subseteq A - \{a\}\}\underline{M}$. Then $(\mathcal{D} \cup \mathcal{D}A^*)\underline{B}$ is equal to the set of $\mathcal{R}$-expressions over the alphabet A .

Proof: Note it is convenient to consider elements of $\mathcal{D}$ as "words" over the alphabet $\{C^*a \mid C \subseteq A - \{a\}\}$. This is reflected in the notation below.

$(\subseteq)$ Let $w \in \mathcal{D}$. If $w = 1$ then w and wA^* can be expressed by the $\mathcal{R}$-expressions ϕ^* and A^* respectively. Otherwise $w = A_1^*a_1 \ldots A_m^*a_m$ where $m > 0$ and $a_i \notin A_i$ for $1 \leq i \leq m$. In this case $w = A_1^*a_1 \ldots A_m^*a_m\phi^*$ and $wA^* = A_1^*a_1 \ldots A_m^*a_mA^*$ which are both $\mathcal{R}$-expressions. Since the set of $\mathcal{R}$-expressions forms a Boolean algebra it contains $(\mathcal{D} \cup \mathcal{D}A^*)\underline{B}$.

$(\supseteq)$ Suppose $w = A_0^*a_1 \ldots a_mA_m^*$, where $m \geq 0$ and $A_{i-1} \subseteq A - \{a_i\}$ for $1 \leq i \leq m$. Clearly, if $A_m = \phi$ then $w \in \mathcal{D}$, and if $A_m = A$ then $w \in \mathcal{D}A^*$, so suppose $\phi \neq A_m \subsetneq A$. Let $w' = A_0^*a_1 \ldots A_{m-1}^*a_m \in \mathcal{D}$.

Claim: $$w = w'A^* \cap \overline{\bigcup_{b \in A - A_m} wbA^*} \ .$$

Let $x \in w$. Clearly $x \in w'A^*$. Now $a_1 \ldots a_m b$ is a subword of all words in wbA^* but, if $b \notin A_m$, $a_1 \ldots a_m b$ is <u>not</u> a subword of x . Therefore $x \notin wbA^*$ for $b \in A - A_m$, that is $x \in \overline{\bigcup_{b \in A-A_m} wbA^*}$. Thus $w \subseteq w'A^* \cap \overline{\bigcup_{b \in A-A_m} wbA^*}$.

Let $x \in w'A^* \cap \overline{\bigcup_{b \in A-A_m} wbA^*}$. Since $x \in w'A^*$, $x = yz$ where $y \in w'$ and $z \in A^*$. Now suppose $\alpha(z) \cap (A - A_m) \neq \phi$. Then $z = ubv$ where $u \in A_m^*$, $b \in \alpha(z) \cap (A - A_m)$, and $v \in A^*$. But this implies $x = yubz \in w'A_m^* bA^* = wbA^* \subseteq \bigcup_{b \in A_m - A} wbA^*$ which is a contradiction. Therefore $z \in A_m^*$, so $x \in w'A_m^* = w$. Thus $w'A^* \cap \overline{\bigcup_{b \in A-A_m} wbA^*} \subseteq w$, and hence the claim is true.

Now for $b \in A - A_m$, $wb \in \mathcal{D}$ and thus $w = w'A^* \cap \overline{\bigcup_{b \in A-A_m} wbA^*} \in (\mathcal{D} \cup \mathcal{D}A^*)\underline{B}$. Since $(\mathcal{D} \cup \mathcal{D}A^*)\underline{B}$ is a Boolean algebra it follows that every $\mathcal{R}$-expression is in $(\mathcal{D} \cup \mathcal{D}A^*)\underline{B}$.

It is now possible to relate the family of languages corresponding to finite $\mathcal{R}$-trivial monoids to the dot-depth hierarchy. That hierarchy is defined by $\mathcal{B}_0 = \{\{a\} \mid a \in A\}\underline{MB}$ and $\mathcal{B}_{i+1} = \mathcal{B}_i\underline{MB}$ for $i \geq 0$.

Since $\{\{a\} \mid a \in A\}\underline{M} = \{\phi^* a \mid a \in A\}\underline{M} \subseteq \{C^* a \mid C \subseteq A - \{a\}\}\underline{M} = \mathcal{D}$ $\mathcal{B}_0 = \{\{a\} \mid a \in A\}\underline{MB} \subseteq \mathcal{D}\underline{B} \subseteq (\mathcal{D} \cup \mathcal{D}A^*)\underline{B}$. Thus all languages in $\mathcal{B}_0$ have finite $\mathcal{R}$-trivial monoids.

Any $_n{\sim}$ language ($_n{\sim}_1$ in the notation of [9]) is also an $_n{\sim}_R$ language. However, the family $\mathcal{B}_1$ is incomparable with our family. The **language $A^*a \in \mathcal{B}_1$, where the cardinality of A is greater than 1, has**

a reduced finite automaton which is not partially ordered. See Fig. 4. In [9, page 116], Simon shows that for the cardinality of A greater than **2 the language denoted by the R-expression a^*bA^* is not in $\mathcal{B}_1$.**

Finally, for any $A_i \subsetneq A$, $A_i^* = \cap\{\overline{A^*aA^*} \mid a \in A - A_i\} \in \mathcal{B}_1$, so that any $\mathcal{R}$-expression denotes a language in $\mathcal{B}_1\underline{MB} = \mathcal{B}_2$.

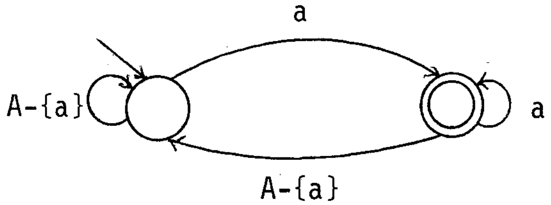

Fig. 4

8. Other Congruences

Besides ${}_n\sim_R$ and ${}_n\simeq_R$ other congruences can be used to characterize the languages corresponding to finite $\mathcal{R}$-trivial monoids.

Definition 33 Let $x,y \in A^*$. Then $x \underset{0}{\leftarrow} y$, and $x \underset{n+1}{\leftarrow} y$ if and only if for each decomposition $x = x'ax''$, with $a \in A$, there exists a decomposition $y = y'ay''$ such that $x' \;{}_n\!\sim y'$ and vice versa.

Definition 34 Let $x,y \in A^*$. Then $x \underset{0}{\overset{\leftarrow}{=}} y$, and $x \underset{n+1}{\overset{\leftarrow}{=}} y$ if and only if for each decomposition $x = x'ax''$, with $a \in A$, there exists a decomposition $y = y'ay''$ such that $x' \underset{n}{\overset{\leftarrow}{=}} y'$ and vice versa.

Definition 35 Let $n \geq 0$ and $x \in A^*$. Then x is n-full if and only if $\mu_n(x) = \cup\{(\alpha(x))^i \mid i = 0,\ldots,n\}$.

Clearly every word is both 0-full and 1-full. One verifies that, for $n \geq 1$, x is n-full if and only if there exist $x_1,\ldots,x_n \in A^*$ such that $x = x_1\ldots x_n$ and $\alpha(x_1) = \ldots = \alpha(x_n)$.

Definition 36 Let $x,y \in A^*$ and $n \geq 1$. Then $x \;{}_n\dot{\equiv}_R\; y$ iff there exist $u,v,z_1,z_2 \in A^*$ such that $x = z_1uz_2$, $y = z_1uvz_2$, u is n-full and $\alpha(u) \geq \alpha(v)$. ${}_n\equiv_R$ is the symmetric transitive closure of ${}_n\dot{\equiv}_R$.

Definition 37 Let $x,y \in A^*$ and $n \geq 1$. Then $x \;{}_n\dot{=}_R\; y$ iff there exist $u,v,z_1,z_2 \in A^*$ such that $x = z_1uz_2$, $y = z_1uvz_2$, u is n-full and $\alpha(u) = \alpha(v)$. ${}_n=_R$ is the symmetric transitive closure of ${}_n\dot{=}_R$.

These various congruences are related as illustrated in Fig. 5. Proofs of these results can be found in [5].

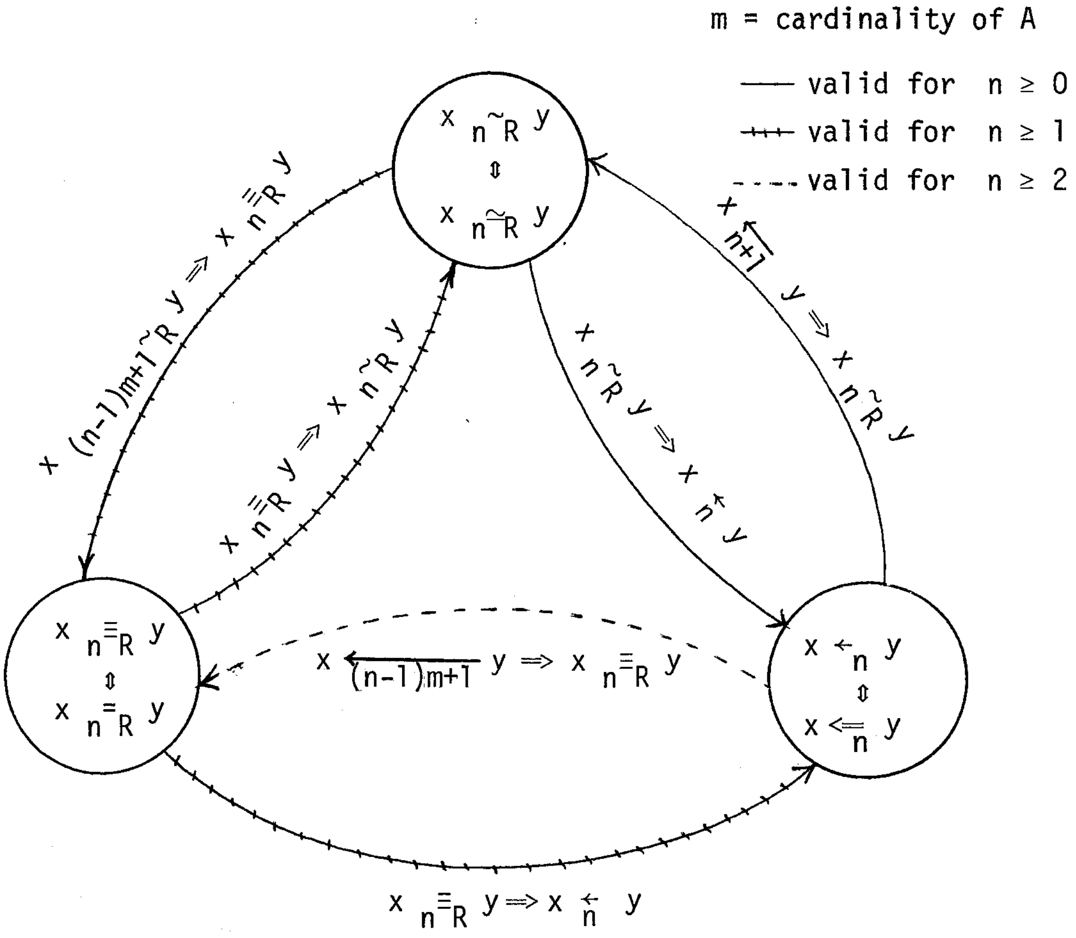

Fig. 5

9. Summary

Theorem 38 Let $X \subseteq A^*$ be a regular language, let M be its syntactic monoid, and let $\underset{\sim}{A} = \langle A, Q, q_0, F, \sigma \rangle$ be the reduced automaton accepting X . The following conditions are equivalent.

M1. M is $\mathcal{R}$-trivial.

M2. For all $f,g,h \in M$, $fgh = f$ implies $fg = f$.

M3. For all idempotents $e \in M$, $eM_e = e$.

M4. There exists an $n > 0$ such that for all $f,g \in M$, $(fg)^n f = (fg)^n$.

X1. X is an ${}_n\sim_R$ language for some $n \geq 0$.

X2. X is an ${}_n\simeq_R$ language for some $n \geq 0$.

X3. X is an $\underset{n}{\leftarrow}$ language for some $n \geq 0$.

X4. X is an $\underset{n}{\Leftarrow}$ language for some $n \geq 0$.

X5. X is an ${}_n\equiv_R$ language for some $n \geq 1$.

X6. X is an ${}_n=_R$ language for some $n \geq 1$.

E1. X can be denoted by an $\mathcal{R}$-expression.

E2. $X \in (\mathcal{D} \cup \mathcal{D}A^*)\underline{B}$ where $\mathcal{D} = \{C^*a \mid C \subseteq A - \{a\}\}\underline{M}$.

A1. $\underset{\sim}{A}$ is partially ordered.

A2. For all $x,y \in A^*$ and for all $q \in Q$, $\sigma(q, xy) = q$ implies $\sigma(q, x) = q$.

A3. $\underset{\sim}{A}$ is covered by a cascade product of half-resets.

10. Languages of $\mathcal{L}$-trivial Monoids

The $\mathcal{L}$-trivial property is dual to that of $\mathcal{R}$-trivialness. As a result, characterizations analogous to those in Theorem 38 hold.

Definitions for the corresponding congruences are formed by using suffixes in place of prefixes. More precisely if $x, y \in A^*$ and $n \geq 0$ then $x \; {}_{n}{\sim}_{L} \; y$ if and only if for each suffix u of x there exists a suffix v of y such that $u \; {}_{n}{\sim} \; v$ and vice versa. The five other congruences (${}_{n}{\simeq}_{L}$, $\underset{n}{\rightarrow}$, $\underset{n}{\Rightarrow}$, ${}_{n}{\equiv}_{L}$, and ${}_{n}{=}_{L}$) have similarly modified definitions.

If $\underset{\sim}{A}$ is the finite automaton of a language with an $\mathcal{L}$-trivial syntactic monoid then $\underset{\sim}{A}^{\rho}$ is partially ordered. However it is possible to describe these automata more directly.

Lemma 39 Let $S = \langle A, Q, \sigma \rangle$ be a semiautomaton, let $x \in A^*$ and let $B \subseteq A$. If $\sigma(q, ax) = \sigma(q, x)$ for all $a \in B$ and all $q \in Q$ then $\sigma(q, wx) = \sigma(q, x)$ for all $w \in B^*$ and all $q \in Q$.

Proof: By induction on $|w|$.

The result is clearly true for $|w| = 0$. Assume it is true for all words in B^n. Suppose $w \in B^{n+1}$. Then $w = aw'$, where $a \in B$ and $w' \in B^n$, so that $\sigma(q, wx) = \sigma(\sigma(q, a), w'x) = \sigma(\sigma(q, a), x) =$ $= \sigma(q, ax) = \sigma(q, x)$. By induction the result is true for all words in B^*.

Proposition 40 Let $\underset{\sim}{S} = \langle A, Q, \sigma \rangle$ be a semiautomaton and let M be its transformation monoid. The following are equivalent.

1. M is L-trivial.
2. There exists an $n > 0$ such that for all connected subsemiautomata $\underset{\sim}{T} = \langle C, P, p_0, \tau\rangle$ of $\underset{\sim}{S}$ and all n-full words w with $\alpha(w) = C$, $\tau(p, w) = \tau(p', w)$ for all $p, p' \in P$.
3. If $x \in A^*$ then $\sigma(q, x) = \sigma(q, xx)$ for all $q \in Q$ implies $\sigma(q, x) = \sigma(q, ax)$ for all $q \in Q$, $a \in \alpha(x)$.

Proof:

($1 \Rightarrow 2$) Suppose M is L-trivial. By the dual of Lemma 17 there exists an $n > 0$ such that for all $x, y \in A^*$, $x \underset{n}{\sim} yx$ implies $\underline{x} = \underline{yx}$.

Let $\underset{\sim}{T} = \langle C, P, p_0, \tau\rangle$ be a connected subsemiautomaton of $\underset{\sim}{S}$, let $p, p' \in P$, and let w be an n-full word with $\alpha(w) = C$.

Since $\underset{\sim}{T}$ is connected there exist $u, v \in C^*$ such that $\tau(p_0, u) = p$ and $\tau(p_0, v) = p'$. Now w is n-full and $u, v \in (\alpha(w))^*$ so $uw \underset{n}{\sim} w$ and $vw \underset{n}{\sim} w$. This implies that $\underline{uw} = \underline{w} = \underline{vw}$ and thus

$\tau(p, w) = \tau(p_0, uw) = \sigma(p_0, uw) = \sigma(p_0, vw) = \tau(p_0, vw) = \tau(p', w)$.

($2 \Rightarrow 3$) Suppose $x \in A^*$ is such that $\sigma(q, x) = \sigma(q, xx)$ for all $q \in Q$. By induction it follows that $\sigma(q, x) = \sigma(q, x^n)$ for all $q \in Q$ and $n \geq 1$.

Let $q \in Q$ and let $a \in \alpha(x)$. Consider the connected subsemiautomaton $\underset{\sim}{T} = \langle\alpha(x), P, q, \tau\rangle$ of $\underset{\sim}{S}$. Since x^n is n-full $\sigma(q, x) = \sigma(q, x^n) = \tau(q, x^n) = \tau(\tau(q, a), x^n)$
$= \sigma(\sigma(q, a), x^n) = \sigma(\sigma(q, a), x) = \sigma(q, ax)$.

(3 $\Rightarrow$ 1) Let $e \in M$ be idempotent and let $g \in P_e$. Let $f,h \in M$ be such that $e = fgh$. Since M is the transformation monoid of $\underset{\sim}{S}$ there exist $x,y,z \in A^*$ such that $\underline{x} = f$, $\underline{y} = g$, and $\underline{z} = h$. Let $w = xyz$ so that $\underline{w} = \underline{xyz} = fgh = e$.

Since e is idempotent $\underline{w} = e = e^2 = \underline{w}^2$ so $\sigma(q, w) = \sigma(q, ww)$ for all $q \in Q$. Therefore $\sigma(q, aw) = \sigma(q, w)$ for all $a \in \alpha(w)$, $q \in Q$. Because $\alpha(y) \subseteq \alpha(w)$ we have, by Lemma 38, that $\sigma(q, yw) = \sigma(q, w)$ for all $q \in Q$. Thus $ge = \underline{yw} = \underline{w} = e$ so $P_e e = e$. But $P_e e = e$ implies $M_e e = e$; hence M is L-trivial.

The final theorem, analogous to Theorem 38, summarizes the characterizations of languages with L-trivial monoids.

Theorem 41 Let $X \subseteq A^*$ be a regular language, let M be its syntactic monoid, and let $A = \langle A, Q, q_0, F, \sigma \rangle$ be the reduced automaton accepting X . The following conditions are equivalent.

M1. M is L-trivial.

M2. For all $f,g,h \in M$, $hgf = f$ implies $gf = f$.

M3. For all idempotents $e \in M$, $M_e e = e$.

M4. There exists an $n > 0$ such that for all $f,g \in M$, $g(fg)^n = (fg)^n$.

X1. X is an ${}_{n}{\sim}_{L}$ language for some $n \geq 0$.

X2. X is an ${}_{n}{\simeq}_{L}$ language for some $n \geq 0$.

X3. X is an $\underset{n}{\rightarrow}$ language for some $n \geq 0$.

X4. X is an $\underset{n}{\Rightarrow}$ language for some $n \geq 0$.

X5. X is an ${}_n\equiv_L$ language for some $n \geq 1$.

X6. X is an ${}_n=_L$ language for some $n \geq 1$.

E1. X can be expressed as the finite union of regular expressions of the form $A_0^* a_1 A_1^* \ldots a_m A_m^*$ where $m \geq 0$, $a_1, \ldots, a_m \in A$ and $A_i \subseteq A - \{a_i\}$ for $1 \leq i \leq m$.

E2. $X \in (\mathcal{D} \cup A^*\mathcal{D})\underline{B}$ where $\mathcal{D} = \{aC^* \mid C \subseteq A - \{a\}\}\underline{M}$.

A1. $\underset{\sim}{A}^\rho$ is partially ordered.

A2. If $x \in A^*$ then $\sigma(q, x) = \sigma(q, xx)$ for all $q \in Q$ implies $\sigma(q, x) = \sigma(q, ax)$ for all $q \in Q$, $a \in \alpha(x)$.

A3. There exists an $n > 0$ such that for all connected subsemiautomata $\underset{\sim}{T} = \langle C, P, p_0, \tau \rangle$ of $\underset{\sim}{A}$ and all n-full words w with $\alpha(w) = C$, $\tau(p, w) = \tau(p', w)$ for all $p, p' \in P$.

A4. $\underset{\sim}{A}^\rho$ is covered by a cascade product of half-resets.

References

[1] J.A. Brzozowski, A generalization of finiteness, Semigroup Forum 13 (1977), 239-251.

[2] A. H. Clifford and G.B. Preston, The Algebraic Theory of Semigroups I, Amer. Math. Soc., Providence, R.I., 1961 .

[3] R.S. Cohen and J.A. Brzozowski, Dot depth of star-free events, J. Comput. System Sci. 5 (1971), 1-16.

[4] S. Eilenberg, Automata, Languages, and Machines, B, Academic Press, New York, 1976.

[5] F.E. Fich, Languages of $\mathcal{R}$-Trivial and Related Monoids, M. Math Thesis, Dept. of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, 1978.

[6] J.A. Green, On the structure of semigroups, Annals of Math. 54 (1951), 163-172.

[7] A.R. Meyer and C. Thompson, Remarks on algebraic decomposition of automata, Math. Systems Theory 3 (1969), 110-118.

[8] M.P. Schützenberger, On finite monoids having only trivial subgroups, Inform. Contr. 8 (1965), 190-194.

[9] I. Simon, Hierarchies of events with dot-depth one, Ph.D. thesis, Dept. of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, 1972.

[10] I. Simon, Piecewise testable events, in Lecture Notes in Computer Science 33, Springer-Verlag, New York, 1975.

[11] P.E. Stiffler, Jr., Extensions of the fundamental theorem of finite semigroups, Advances in Mathematics 11 (1973), 159-209.

[12] Y. Zalcstein, Remarks on Automata and Semigroups, unpublished (1971).